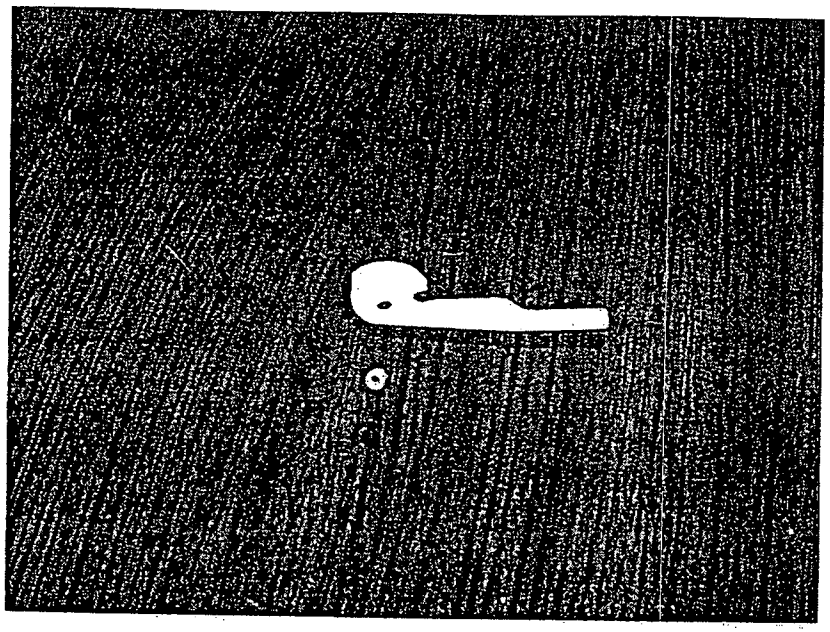
Computer system pre-boot security detection method for detecting invalid operation code

Patent Number:
Publication date: 2001-12-01
Inventor(s): TSAI JIUN-NAN (TW)
Applicant(s): MITAC INTERNAT CORP (TW)
Requested Patent: TW466402
Application Number: TW19990117201 19991006
Priority Number(s): TW19990117201 19991006
IPC Classification: G06F11/30
EC Classification:
Equivalents:

Abstract

There is provided a computer system pre-boot security detection method for detecting invalid operation code that executes computer pre-boot security system by detecting invalid operation code in the program to trigger the interrupt service function of the interrupt vector INT 6 of the microprocessor. This method saves the vector address of the original interrupt vector INT 6 of the microprocessor after the computer system power is on and the microprocessor executes power on self-test. Then, a group of new interrupt service programs are set to execute system security check. After executing an invalid operation code, it activates the new interrupt vector function to execute security checking steps. It executes the normal computer system boot step if the system security check is passed, or locks keyboard operation if the system security check is not passed.



Disclosed by International Business Machines Corporation
42775

42776

Network Connect Detection Using Alert-on-LAN

Power on Self Test software installed on all computer systems are increasingly asked to do more tasks in a shorter amount of time. One of these tasks is the retrieval and display of a network interface card's (NIC's) MAC address. This address is obtained from a function call to the NIC. The problem arises when a system is not connected to a network. According to a strict interpretation of the MAC address specification, the NIC needs to be connected to the network in order to respond with a valid MAC address. There are some NICs that do not adhere so strictly to the specification and return the MAC address whether or not they are connected, however, we have run into some specific examples of cards that do respond strictly to the specification. This may not seem like a problem until you consider that a NIC will not know that it is not connected to a LAN until twenty seconds has elapsed without a response. Waiting twenty seconds for the MAC address during POST while the total POST time is suposed to be less then thirty seconds is not an acceptable solution. What is needed is a way of knowing whether or not we are physically connected to a LAN before we ask for the MAC address.

This new invention utilizes the Alert-on-LAN in a manner that it was never intentionally meant to run. Additionally, no hardware change is required for this invention to be implemented. When sending an AoL packet, the status registers indicate whether or not the packet has been sent. In order for the status bit to clear, the packet has to be sent and received by a server. If the system is not connected to the network, the status will never clear. We can use this status bit to reduce the amount of time it takes to detect the presence of a network. By sending a broadcast packet across the network, the first system that receives the packet will respond and cause the send bit to clear. We can set the time-out time to a more reasonable value. With this method it is estimated that we can reduce the network not present time from 20 seconds down to about 2 seconds. A 10x Savings in POST time!

Disclosed by International Business Machines Corporation
42776